Cyber Security Solutions for Small and Mid Sized Businesses

A practical guide to defending your company against cyberattacks

Are You Prepared?

CRESCENT IT SYSTEMS

VIPRE, a security product company, recently commissioned a survey of 250 SMB IT managers which found that:

- ***23 percent of the respondents reported that they experience cyberattacks daily.***
- ***66 percent indicated they would either go out of business or shut down fora day or more if systems and/or data are compromised.***
- ***47% report they have to manually collect data for their security reports to management.***

Types of Cyberthreats:

Small and mid sized business are especially targeted by cybercriminals for their statistically lower expenditures on cybersecurity. Lawsuits and penalties for breach of personal information can add up to 6-10+% of a company's gross revenue according to James Morrison, Cyber Expert with the Houston FBI office. The following are the most common cyberthreats to defend against.

Malware:

Malware is a software designed to do one or many roles such as inflict downtime, infect other company systems with nefarious intent, damage or steal information.

Ransomware:

Ransomware is a malware that infects, encrypts and locks data on systems and demands a ransom of money, in return, to provide the password or key to restore the data.

Business Email Compromise (BEC):

Cybercriminals will send a email formed to look like it was sent within the company to fool the employee in revealing sensitive information. Other "Social Engineering" tricks include telephone calls with a caller id indicating an in-house company call.

Trojans:

A hacker will gain control of remote computers by sending a malicious link to an employee who will open from a website or email. The malicious link will install malware onto the computer and allow access to the hackers to perform unauthorized access and activity on the company network.

Keyloggers:

Keyloggers are especially dangerous in that they are usually deployed from malicious email or web links and run silently in the background with the sole purpose of obtaining for banking or financial login information.

Cyber Security Solutions

Strategy Planning for the Cyberthreats

1. Identify your current cyber defense status. Select key employees from each department to gain a 360 degree view of your current security. The IT employees may be heavily involved in the security, but the company's data may be assessible to the wrong employees. Probing questions to ask:

    - Who is in charge of security and what exact measures are in place?
    - Are their specific responses already planned in the event of a breach? If not, then list the exact weaknesses in the cyber defenses.
    - Has there been a file permissions audit of the data to ensure the authorized employees are the only ones that can access the data.
    - Are the current IT security policies in compliance with the regulatory requirements for the company for its given industry?

2. If a chief security officer (CSO) is not assigned, then one should be appointed. A Chief Security Officer (CSO) is responsible for the physical security of a company, including its communication and business systems. The CSO is to protect people, assets, infrastructure and technology and is responsible for the security strategy.

3. Each function of the company must be reviewed and a decision must be made to either handle the security internally or outsource to a specialized vendor to ensure the safety of the company data. For example, there may be a number of HR web vendors to outsource to that would take the responsibility of the security of the HR data. The same goes for accounting and payroll and other functions.

4. A number of assessments and inventories should be performed to determine the current status. The following are just a few of the assessments to be done:

    - A data permissions audit must be performed if one has not been performed in the last 6 months.
    - An inventory of the technology assets must be taken and a priority of value to cybercriminals in regards to each asset must be assigned. Assign a value to each asset in regards to ease of availability and confidentiality.

(281) 358-3589 www.crescent-systems.com

CRESCENT IT SYSTEMS

Implementing Your Cyber Defense Plan

Company policies and employee actions are the main resources to combat cyber crime and to maintain the confidentiality of the company data. The policies sets the critical employee expectations needed for ensuring the company's data is secured. Training of the employees to reinforce the company's security goals will ensure that the employees know what is expected.

1. Training: Security Specialists recommend the following to effectively train your employees:

- Train the employees and affirm the basic company expectations of secure passwords, use of business assets in a safe manner in utilizing the internet as well as secure handling of the company data.
- Continue to train your employees with common "Social Engineering" ploys used to gain access to sensitive company data or assets.
- Annual or more frequent training should be done.

2. Implementation: Given your earlier assessments and inventories, ensure that the following are done:

- The data permissions audit is reviewed and the appropriate changes to limit the employee access to the data that is appropriate for their position.
- Update the company policies with employee expectations of how the business assets are to be used. An Acceptable Use Policy should be part of the company policies to draw the line of how the employees use the business resources.
- Establish periodic meetings to review the current status of security or changes to the workflow of data or vendors to ensure of the proper access.
- Employ an external IT security consultant to review and assess your environment.
- Ensure that your IT security policies are documented, up to date and covers the regulatory requirements for your industry.

3. Data Protection: Backing up the data to multiple locations and frequently verifying the backups for successful capture is critical. The job to ensure that the data is being backed up reliably is assigned to one or more employees.

4. Patch/Update Management: All computer and network systems should have their vendor patches applied when available.

CRESCENT IT SYSTEMS

Tools & Solutions to Combat Cyber Crime

Security should be viewed like a medieval kingdom with layers of protection. The medieval kingdom will have a moat to restrict the raiders from having easy access to the castle walls. There is a drawbridge that allows authorized access to those they deem worth of entering the castle. There is hot tar to throw over the wall to defend against those who attempt climbing the walls. The high walls are used to impose a huge obstacle to stop invaders. The "keep" of the castle is used to hold the valuables of the kingdom where there are thick walls and strong steel doors.

The same goes for network security where the layers of protection should be used. A firewall which blocks external users for access, the anti-virus software that blocks infections on computer systems, and data permissions restricts the access to those that are authorized.

There are a number of industry best practices for businesses to use.

- The firewall is the oldest and most basic network security function. Firewalls restrict the establishment of network connections between hosts inside and outside the organization with the intention of reducing or eliminating exposure to external hosts, networks or protocols that are known to be vectors for network threats.
- A Unified Threat Management appliance offers multiple layers of security which provides the basic firewall capabilities, but in addition it protects networks against combined security threats, including malware, SPAM, Virtual Private Network access and attacks that simultaneously target separate parts of the network.
- Anti-Virus solutions protect against most virus attacks.
- Data backup software to recover lost or corrupted data.
- Encryption software can protect data no matter where it is stored.
- Password security software provides better passwords and prevents password cracking along with frequent password changes.
- Two-step authentication (2FA) can help in authenticating the user to ensure the authorized user is actually accessing the data.
- Biometric login devices are an extra step in ensuring that the right user is accessing the data.

Again, security is a layered protection sphere around your company and its data.

Tools & Solutions to Combat Cyber Crime

There are a number of ways to protect yourself from various cyber attacks that involve your employees and their responses to various malware attacks as follows:

1. **Online Banking Malware:** This will steal a user's login into a financial institution. According to a SCORE survey in 2017, 71% of the customers use online banking with 43% using mobile banking websites. A cybercriminal can make use of a login information captured within 9 minutes.
   Protect against a Banking Malware with the following:
   - Directly type a bank's website as a precaution.
   - Use additional authentication software like Trusteer or two factor authentication.
   - Use bookmarked trusted websites
2. **Macro Malware:** Microsoft files utilize macros that are like small programs that can perform a set of functions. Cybercriminals rewrite these macros to do nefarious actions and can be sent as email attachments, and when opened they deploy their malware payload into the computer system and network it is on. The majority of the emails were SPAM emails.
   Protect against a Macro Malware by:
   - Employ a SPAM solution like a software or a Unified Threat Management appliance to prevent SPAM with malicious payloads from getting to the user.
   - Disable macros in Microsoft applications.
   - Check for misspelled words within a email that might indicate a hack.
   - Do not open a attachment from someone you do not know. Symantec's 2019 Internet Security Threat Report stated that 48% of malicious email attachments were in email attached Microsoft Office files.
3. **Ransomware:** Ransomware often downloads and deploys malware that locks the data until a payment is made.
   Protect against a Ransomware by:
   - Avoid opening emails from unknown sources or with embedded weblinks or unusual attachments.
   - Frequently update your anti-virus, anti-SPAM software and promptly apply vendor patches to patch vulnerabilities.
   - Also be suspicious of "urgent" emails that demands immediate action.

CRESCENT IT SYSTEMS

"Small businesses are considered rich targets for cybercrime today."
James Morrison, a Houston FBI Computer Scientist, speaking about Cybersecurity at the West Houston Chamber Cybersecurity event on August 2nd framed the danger to small to mid sized businesses today.

Morrison stated, "*The mindset of the cyber criminals is different than normally think. It is not what they can steal from you, but it is what so important to you, that you will pay them to get it back."*

Morrison adds; "*Many states have privacy laws and if you lose someone's data, you are going to be sued.*"

All businesses need to take action in shoring up their cyber security measures ASAP to prevent the financial and legal consequences of a cyber crime.

Crescent IT Systems has been providing stress-free IT support for its clients for over 24 years with our experienced and caring consultants.

Call today to learn more of what to do to protect your company against Cyber Crime with our free assessment.

www.crescent-systems.com - (281) 358-3589
pegarrison@crescent-systems.com * 9600 Long Point Rd., Suite 228, Houston TX 77055